Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

March - April 2024

This page is intentionally left blank

INTRODUCTION

For period 1st March - 30th April

Welcome to the latest edition of the Cyber Threat Update brought to you by the Cyber Security Centre for the Isle of Man (CSC), a part of OCSIA. This document provides an overview of cyber threats using data collected from our reporting points as well as intelligence obtained from partner agencies and open-source services.

We can only offer advice and guidance based on the information we have. Therefore, if you have any information that you believe should be considered for this document, please reach out to us at cyber@gov.im or submit it via our online cyber concerns form.

CONTENTS

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

As part of the Isle of Man Government's Cyber Security Strategy, the Cyber Security Centre for the Isle of Man (CSC) operates a Suspicious Email Reporting Service (SERS), allowing residents to forward suspicious emails for analysis.

If you have received an email which you're not quite sure about, forward it to SERS@ocsia.im. The message might be from a company that you don't normally receive communications from or from someone that you do not know. You may just have a hunch. If you are suspicious about an email, you should report it.

Your report of a phishing email will help us to act quickly, protecting many more people from being affected. In a small number of cases, an email may not reach our service due to it already being widely recognised by spam detection services.

By sending your suspicious emails to us we can better understand the threats on our Island and provide relevant advice and warnings. Your email will also be analysed by the UK's National Cyber Security Centre (NCSC), assisting in the disruption of malicious phishing campaigns and take down of websites.

The National Cyber Security Centre (NCSC) has the power to investigate and remove scam email addresses and websites. By reporting phishing attempts you can:

- reduce the amount of scam emails you receive
- make yourself a harder target for scammers
- protect others from cyber crime online

Since the launch of SERS, we have received over 19,343 suspicious emails. In March and April 2024, we received 1,031 suspicious emails.

SUSPICIOUS EMAILS

1,031 REPORTED

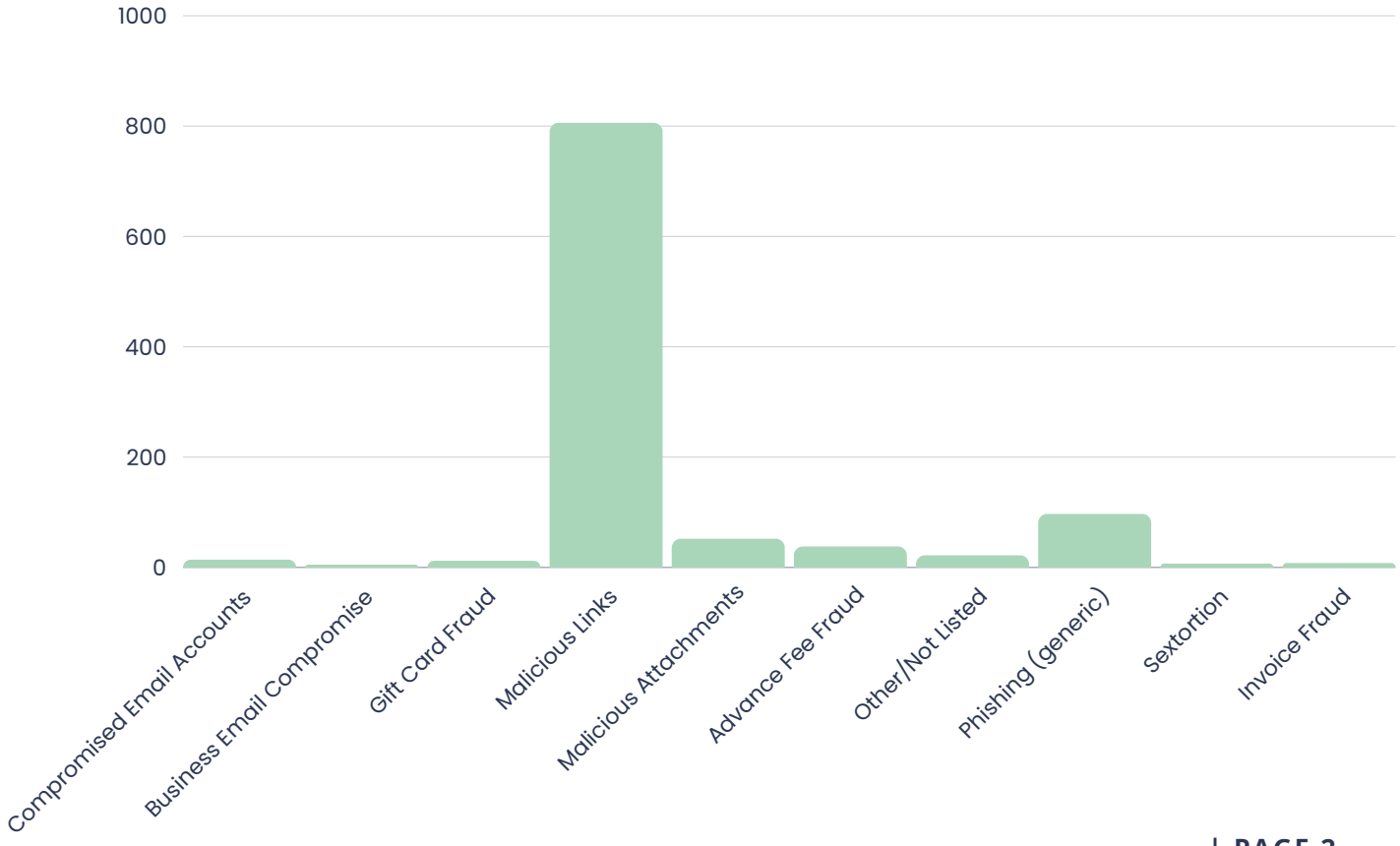
in March & April

Detail

The chart (below) details the type of emails sent by cybercriminals that have been reported to our SERS for the months of March and April. Whilst the infographic (right) showcases the top five most impersonated companies and services.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Parcel Delivery
3. Apple
4. Retail Stores
5. Anti-virus software



CYBER CONCERNS

83 REPORTED

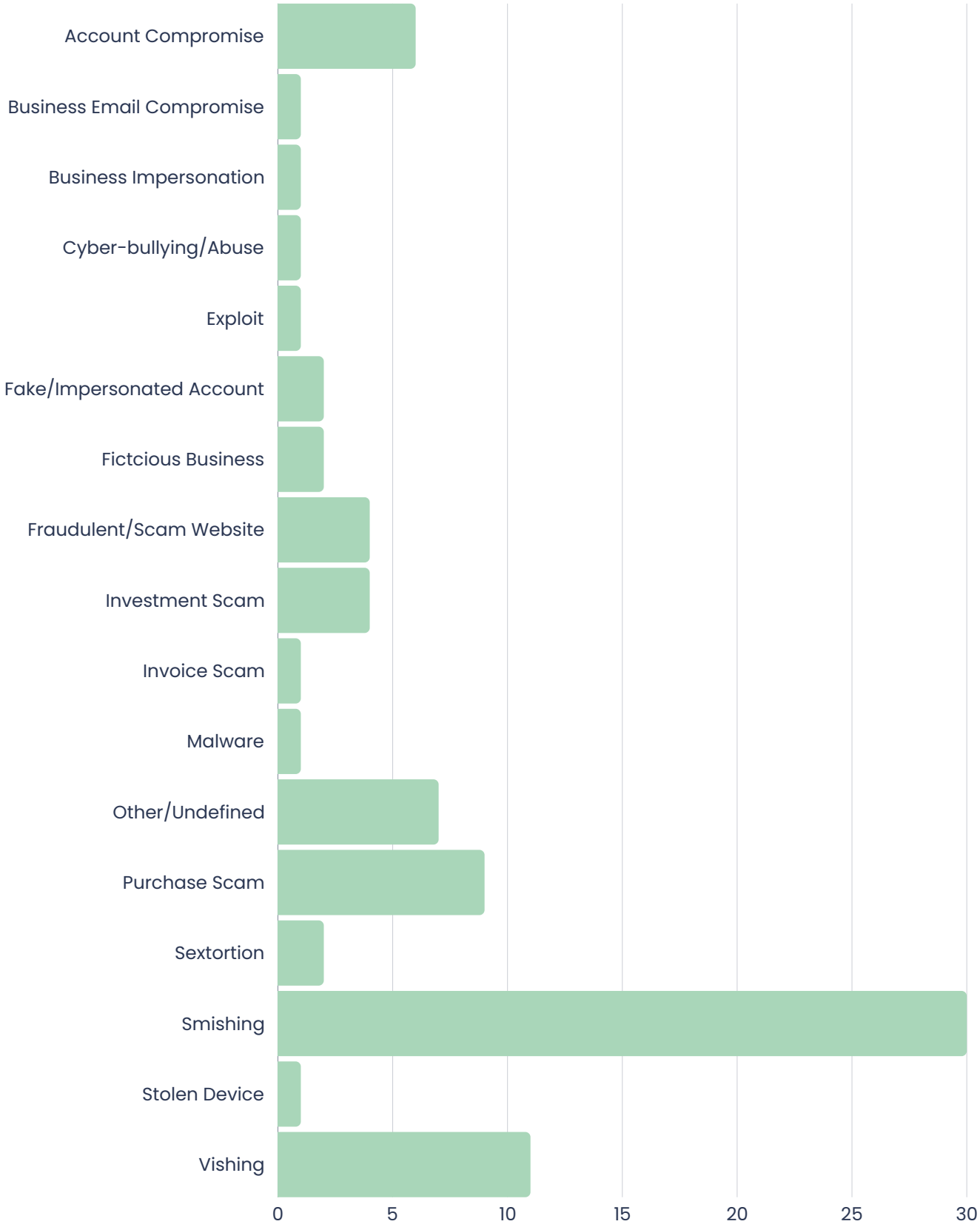
in March and April

Detail

The chart (on page 4) shows a breakdown of cyber concerns reported to us over March and April.

As mentioned previously, we can only provide the right advice and guidance to the public and local businesses from the information that is shared and reported to us. It is, therefore, important that we receive reports from the public and from organisations. If anyone has any information that they wish to put forward for consideration that could contribute to this document, please contact us at cyber@gov.im or report it using our online cyber concerns form.

Cyber Concerns March & April



ISLE OF MAN THREAT COMMENTARY

BUSINESS EMAIL COMPROMISE

GOVERNMENT DEPARTMENT

A government department reported an instance of business email compromise, where a member of staff has been impersonated and requested to change their bank details. The criminal was described by the reporter as 'very pushy' and proceeded to request a copy of the employee's latest payslip.

Alarm bells rang in HR, prompting them to contact the involved member of staff in person, to discuss whether or not this was a legitimate request or if their email account could have been compromised. On confirmation from the employee that they had not asked to change their bank details, the reporter contacted the CSC to report the incident.

Bank details provided by the scammer were noted down and passed onto law enforcement agencies, who then took over the investigation on a criminal level.

The CSC provided details for securing the compromised account, including reporting the incident to the relevant IT team and to forward the emails sent from the compromised address to us at SERS@ocsia.im for logging purposes.

This incident highlights the importance of good password security and the implementation of MFA, as a way to reduce the risk of business email compromise. It is also imperative that information posted on websites, like LinkedIn, do not contain anything sensitive that could be used by cybercriminals once they have gained access to a compromised account to make their fraudulent emails more convincing.

GIFT CARD FRAUD

LOCAL RESIDENT HIT BY COMPROMISED ACCOUNT

We were made aware of a resident who received an email from someone she believed to be a friend requesting a £200 Apple gift voucher. This was then purchased, and a code was sent to the victim.

The victim then sent the codes onward to the scammer who immediately redeemed them. The victim was then subsequently asked to purchase another £150 worth of gift cards. It was at this point the victim became suspicious and halted contact with the scammer.

This case emphasises the importance of verifying the authenticity of requests, especially when they involve financial transactions or sensitive information. Even if a request appears to come from a familiar source, taking the time to confirm its legitimacy through alternative means can prevent falling victim to scams. It also underscores the need to remain sceptical of urgency. Scammers often create a sense of urgency to pressure individuals into acting hastily, without considering the potential risks involved. It's essential to pause, assess the situation calmly, and scrutinise requests, particularly when they involve spending money or sharing personal details.

£12,975

Reported financial losses to Gift Card Fraud in 2023, to find out more, check out our Threat Update Annual Report.

MALWARE

LOCAL RESIDENT

A local restaurant had their website reported to us in March when a prospective customer accessed the site and the presence of malware was flagged by his anti-virus software. When the URL was passed through an online-scanning tool, a malicious JavaScript script was highlighted, along with the presence of 12 different vulnerabilities.

We do not know how this website became infected, however, it is possible that one of the found vulnerabilities could have been the entry point. Upon receiving the report, the CSC immediately contacted the restaurant to inform them of their infected domain and recommended that they contacted their website developer to check for any issues and ensure all vulnerabilities are patched.

This story highlights how important it is to ensure your business is secure when operating online. Lessons can be learned by other local service suppliers about regularly applying security updates and patches to their software and not letting their website domains expire, reducing the risk of other websites becoming embedded with malware in the future.

INVESTMENT SCAMS

OVER £125,000 LOST IN THE PERIOD

Investment scams are on the rise and, unfortunately, we have been made aware of around £125,000 being lost over the previous two months. One victim reported a loss of over £85,000 after investing in cryptocurrency through a fake trading platform, while other victims were tricked into investing through false celebrity endorsements including Jeremy Clarkson and Richard Hammond.

The fraudulent trading platforms reported to us in the period were 'Crypto.com Trust', 'Delta-Stock.com', and 'OnePlusCapitalCSD'. Criminals pretending to be traders called the victims multiple times a day and explained how to withdraw any investment profits generated funds the victim must first deposit more money.

The majority of investment scams reported to us during the period involved the installation of remote-access software known as AnyDesk, which cybercriminals can use to monitor their victim's digital activity. This software can be particularly dangerous as it can lead to password compromise, malicious use of stolen digital certificates, and potential supply chain attacks.

Investment scams are nothing new, but they continue to be a profitable attack vector for cybercriminals to use. Lessons can be learned from these unfortunate reports, as they highlight the importance of not getting involved in any sort of 'Get Rich Quick' schemes and to ignore unrequested investment offers made online, over the phone, or on social media. If you do decide to invest in any sort of cryptocurrency, do your research into the broker or trading platform before parting with funds, and do not download any programs onto your device if requested to by an investor.

SEXTORTION

MANIPULATED IMAGES

Over the period, we saw seven reports of sextortion most of which had a significant emotional impact on their victims.

In one case, an individual and their friends encountered what they believed to be a bot on Instagram. Finding it amusing, they decided to interact with the bot for fun. The bot hinted at exchanging photos, so they took a screenshot from a website and sent it over. Unfortunately, it turned out that this was not a bot but a real person.

The person then demanded £300, threatening to distribute the photos, which had been manipulated, including editing the individual's face on the images, to all of the individual's followers. Additionally, the blackmailer edited the photos to include the individual's face, making the situation appear even more authentic.

This is the second such report we've seen where a criminal has manipulated images in order to 'sextort' a victim. We always advise that recipients who are aware of a scam do not engage with the criminal and this example highlights that better than most. Whilst it may be amusing or feel like you are wasting a scammers time, they are using this to gain more information that may be used in future..

EXTERNAL THREAT COMMENTARY

ANTI-KREMLIN HACKTIVISM GROUP TARGET PRISON DATABASE FOR REVENGE

Following the death of a prominent leader of the opposition held in a Russian prison, a group of anti-Kremlin hackers emerged looking to avenge the deceased. Using an entry point into a computer network associated with the Russian prison system, the group being described as hacktivists plastered the website of a prison-contractor with the image of the deceased, along with a message reading 'Long Live Alexey Navalny!'.

In addition to the website defacement, the hacking group appear to have stolen a database containing information of hundreds of thousands of Russian prisoners, along with their relatives and contacts. While less severe than the data leak, the hacktivists exploited their access to the Russian prison system's online commissary, which is used by family members to purchase provisions for inmates, and reduced the price of items normally greater than $1 to only $0.01 (1 ruble). Shop administrators were slow to notice the drastic price change, causing the prison shop to require three days to fully rectify the hacker-induced discounts.

Hacktivism is quickly becoming a strong force in the cybercrime environment: designed to use hacking techniques for political and social causes, as a way of civil disobedience and leverage of digital tools to protest or take direct action against causes group members believe are wrong.

CYBER ATTACK STRIKES LEICESTER CITY COUNCIL: STOLEN DATA SOLD ON DARK WEB, SERVICES DISRUPTED

Leicester City Council faces a significant cyber threat as hackers breach its systems, with fears rising over the sale of stolen data on the dark web. The incident, which initiated on 7 March, compelled the council to take drastic measures, including the shutdown of phone and computer systems. Reports suggest that a ransomware group named INC Ransom has claimed responsibility, exacerbating concerns over data privacy and security.

Dr Ismini Vasileiou, an expert in information systems from De Montfort University, voiced apprehension regarding the potential exploitation of pilfered data. 'The criminal applications of such data are myriad,' she emphasised, noting the ambiguity surrounding the extent of the breach and its repercussions.

Meanwhile, Richard Sword, Leicester City Council's strategic director of city developments and neighbourhoods, expressed regret over the disruption caused by the cyber incident. Essential services, including child protection and adult social care, were inaccessible, necessitating the publication of emergency contact numbers to mitigate the impacts.

The council's efforts to contain the breach align with a broader trend of increasing cyberattacks targeting local authorities, as highlighted by the Information Commissioner's Office. Such assaults not only disrupt services but also pose substantial risks to data security and public trust.

In a concerning development, confidential documents stolen from the council's servers have surfaced online, including sensitive information such as rent statements and passport details. Oliver Spence, CEO of cybersecurity firm Cybaverse, warned of the growing threat posed by ransomware groups like INC Ransom, underscoring the imperative for robust defence mechanisms and employee training.

As investigations continue, Leicester City Council is dealing with the effects of the cyber attack, trying to manage data protection and cybersecurity issues. The incident highlights the ongoing threats from cybercriminals and has led to calls for increased alertness and better measures to protect important systems and sensitive data.

FRENCH HOSPITAL POSTPONES PROCEDURES FOLLOWING CYBERATTACK

The hospital Simone Veil, located in Cannes, France, have announced that they were targeted by a cyberattack on 16 April, severely impacting hospital operations and forcing staff to revert back to using paper records when digital records became inaccessible. Consequently, non-urgent procedures were cancelled, with a limit placed on the hospital to only carry out emergency procedures. While some procedures were carried out successfully, they were only attempted if they were not dependent on computer systems. As of 17 April, when the last update was released by hospital administration, there had not been any ransom demands or data exfiltration observed.

This is the third French hospital to be targeted in 36 months; in December 2022 the Hospital Centre of Versailles was hit with by a cyberattack, and in August 2022 the Center Hospitalier Sud Francilien, a hospital southeast of Paris, suffered a ransomware attack. While all of these attacks are unrelated, the trend highlighted through such attacks on critical national infrastructure shows how important it is for key services to ensure they are applying the most recent, secure cybersecurity mitigation tactics, and the application of system and software updates to patch any known vulnerabilities.

NHS DUMFRIES AND GALLOWAY TARGETED BY RANSOMWARE ATTACK

Back in March it was revealed that a ransomware group of cyber-extortionists had stolen patient data from Scottish hospital NHS Dumfries and Galloway. In a bid to demand money from the local health board, the adversary published an excerpt of stolen data to their dark web blog alongside a warning that more confidential data would be released if ransom demands were not met. Attribution of the attack has not yet been connecting the attack to a specific adversary.

Days after the attack Scotland's Health Secretary tried to reassure patients and staff, but warned that 'those responsible may have acquired a significant of information including patient and staff-specific information'. The health board urged the public to stay vigilant about any potential approach by someone claiming to be in possession of either their personal data or NHS data, and announced that they would be contacting all those with personal data involved in the leak. Work has begun to take place with partner agencies, including Police Scotland, the National Cyber Security Centre and the Scottish Government, to assess the published data.

Attacks on British organisations have increased year-on-year since 2019. Around the time of the attack, the British government was accused by a parliamentary committee of taking the 'ostrich strategy' by burying its head in the sand over the 'large and imminent' national cyber threat posed by ransomware.

VULNERABILITY IN PALO ALTO NETWORKS PAN-OS SOFTWARE EXPOSES THOUSANDS OF FIREWALLS TO ATTACKS

A critical vulnerability, tracked as CVE-2024-3400, has been identified in Palo Alto Networks PAN-OS software, affecting roughly 6,000 internet-accessible firewalls worldwide. Cyber-attackers have been exploiting this vulnerability since late March, posing a significant risk to organisations globally.

Victims of cyber-attacks has recently included an Isle of Man-based company where evidence of hacking and the use of bespoke exploitation tools have been discovered. Exploitation of this flaw, primarily targeting the GlobalProtect feature, allows attackers to execute arbitrary code with root privileges, potentially leading to full system compromise.

Palo Alto Networks has released patches for affected versions, emphasising the urgency of upgrading to prevent further exploitation.

The flaw was discovered by security firm Volexity on 10 April, during an investigation into suspicious traffic from a compromised firewall. Identified as UTA0218, the threat actor swiftly deployed exploits, indicating sophisticated tradecraft and rapid lateral movement within victim networks.

Palo Alto Networks has released patches for affected PAN-OS versions, including PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, and PAN-OS 11.1.2-h3, among others. These patches aim to prevent remote command execution and thwart post-exploitation activities by attackers.

The UK'S National Cyber Security Centre (NCSC) advises organisations to prioritise installing these updates and follow vendor best practices for mitigation. Organisations that use PAN-OS GlobalProtect gateway and portal are urged to monitor the vendor's security advisories closely and implement security updates once available for their version. Continuous monitoring and threat hunting activities are recommended to detect and respond to potential compromises.

In the event of a suspected compromise, organisations in the Isle of Man are encouraged to report incidents to the Cyber Security Centre for further assistance.

CYBER GLOSSARY

Anti-virus software: Designed to identify and remove computer viruses, other malware and spyware on a device or IT system. To be effective, it should be kept up-to-date with the latest anti-virus signatures and definitions.

Backdoor: A backdoor is a method of avoiding normal authentication on a device. They are often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems

Common Vulnerabilities and Exposures (CVE): The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Cryptocurrency: A cryptocurrency is a digital asset that is designed to act as an exchange medium. They use cryptography to verify and secure transactions, control the creation of new assets and protect the identity of asset holders.

Dark web: A collection of thousands of websites which are not indexed by conventional search engines. They often use anonymity tools, like the Tor network, to hide their IP address and preserve the anonymity of the creators and visitors.

Encryption: A method to scramble a message, file or other data and turn it into a secret code using an algorithm (complex mathematical formula). The code can only be read using a key or other piece of information (such as a password) which can decrypt the code.

Firewall: A security system that monitors and controls traffic between an internal network (trusted to be secure) and an external network (not trusted). It is generally considered insufficient against modern cyber threats.

General Data Protection Regulation - GDPR: The General Data Protection Regulation (GDPR) 2016/679 is a European Union regulation covering data protection and individual privacy rights. It was introduced in April 2018 and enforced on May 25 2018.

Hacker: A hacker is a computer and networking attacker who systematically attempts to penetrate a computer system or network using tools and attack methods to find and exploit security vulnerabilities.

IP address: An IP address (Internet Protocol Address) is a label assigned to computer devices. An IP address is essential for Internet Protocol communication.

Keylogging: Keylogging, also known as keystroke logging or keyboard capture, is the action of recording, often secretly, the keys struck on a keyboard.

Malware: Malware is malicious or hostile software used to disrupt, damage or compromise a computer system or network

Patch management: Patch management covers acquiring, testing and installing multiple patches (manufacturer released code changes) to a computer system or application. Firmware and software vendors release patches to fix defects, change functionality and to address known security vulnerabilities.

Phishing: Phishing is a type of fraud in which the attacker attempts to steal sensitive data such as passwords or credit card numbers, via social engineering.

Ransomware: A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker.

Smishing: A type of phishing attack that uses text messages (or other types instead of mobile messaging such as MMS or IM services) instead of email messages.

Social engineering: An attack method that tricks people into breaking normal security procedures by masquerading as a reputable entity or person in email, IM or other communication channels.

Vulnerability: A vulnerability is a weakness that allows an attacker to compromise security (integrity, confidentiality or availability).

CLICK HERE OR SCAN TO VIEW OUR FULL CYBER GLOSSARY

ABOUT US

The Cyber Security Centre for the Isle of Man (CSC) was launched as a branch of the Office of Cyber Security and Information Assurance (OCSIA) in October 2023, to increase our presence in the public sphere. The CSC is responsible for providing targeted advice and guidance to individuals and businesses, while OCSIA remains for Information Assurance within Government.

Our objective is to improve cyber resilience of everyone who lives or operates in the Isle of Man. Our commitment to supporting individuals, businesses and the private sector is at the heart of what we do, and we are devoted to maintaining partnerships with everyone who needs us, while raising awareness about the rapidly changing cybersecurity threat landscape.

Established in 2019, our annual one-day cybersecurity conference ‘CYBERISLE’ takes place in autumn, and acts as a focal point event in the field on Island. We bring together leading experts, students, charities and individuals, to share ideas and allow everyone to gain a deeper understanding of current cyber threats to our Island, and the best mitigation tactics available for increasing nationwide cyber resilience.

CYBERISLE 2024

The Island's premier cyber security conference returns in October for what will be its sixth year, providing guidance on how to prepare for, respond to and recover from any potential cyber incidents for individuals and organisations alike.

Previous conferences have featured a range of speakers including representatives from the National Cyber Security Centre – part of the UK Government Communications Headquarters (GCHQ) – and industry experts. This instalment will build upon the messages from previous years so that business leaders, community groups, charitable organisations and private individuals can work together to keep the Isle of Man's cyberspace safe.

'We are continuing to see high profile cyber-attacks affect both organisations and governments globally,' said Minister for Justice and Home Affairs Hon Jane Poole-Wilson MHK. 'It's important we continue to raise awareness and help equip individuals and organisations with the knowledge to counter these threats.'

CYBERISLE is organised by the Cyber Security Centre (CSC) for the Isle of Man, a part of OCSIA, and the Department of Home Affairs. The event is supported through sponsorship and aims to be run on a cost-neutral basis.

Do you have a topic you wish to share your knowledge on? CYBERISLE is looking for speakers and panellists. If you wish speak at CYBERISLE please email cyberisle@gov.im with a brief overview of your topic.

Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

Cyber Security Centre for the Isle of Man
a part of the Office of Cyber-Security & Information Assurance

csc.gov.im
cyber@gov.im
01624 685557

Office of Cyber-Security & Information Assurance
2nd Floor
Former Lower Douglas Police Station
Fort Street
Douglas
Isle of Man
IM1 2SR

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin